CORRESPONDENCE REGARDING RESUBMISSION OF AMENDMENT	Docket No. L0T9-99-0001

Applicant:	Steven R. Beckhardt, Michael R. O'Brien, Elizabeth A. Lorenson and Douglas W. Conmy
Serial No:	09/431,344
Filed:	October 29, 1999
For:	METHOD AND APPARATUS FOR ENCRYPTING ELECTRONIC MESSAGES COMPOSED USING ABBREVIATED ADDRESS BOOKS
Examiner:	C. Fields
Art Unit:	2766

CERTIFICATE OF MAILING UNDER 37 C.F.R. §1.8(a)

The undersigned hereby certifies that this document is being placed in the United States mail with first-class postage attached, addressed to Mail Stop Non-Fee Amendment, Commissioner for Patents, P.O. Box 1450, Alexandria VA 22313-1450 on August 10, 2004 .

Frances M. Cunningham

Frances M. Cunningham

Mail Stop Non-Fee Amendment
Commissioner for Patents
P.O Box 1450
Alexandria VA 22313-1450

REMARKS

Applicants respectfully request that the Examiner enter the amendment attached hereto as Exhibit A and accord the same the mailing date of March 22, 2004.

Applicants and their attorney wish to thank Examiner Courtney D. Fields for the courtesy of the telephone interviews on August 3, 2004 and August 9, 2004 in which non-receipt of a response to the outstanding office action in the above-identified case was discussed. On August 9, 2004, the Examiner requested resubmission of the attached copies of response along with proof of submission.

On March 22, 2004, Applicant submitted an amendment, a copy of which is enclosed herewith as Exhibit A, in response to the Office Action dated December 23, 2003. This amendment was mailed using a certificate of mailing under 37 CFR 1.8(a), signed by Brenda A. Kantorski, and, therefore, is entitled to a filing date of March 22, 2004. A copy of Applicant's Transmittal Letter that accompanied the Amendment is

enclosed herewith as Exhibit B. A copy of Applicant's return postcard, date stamped March 25, 2004 by the USPTO, is enclosed herewith as Exhibit C, and evidences the USPTO's receipt of the Amendment, Transmittal Letter and a Certificate of Mailing. The postcard further lists the serial number as "09/431,344", the USPTO serial number of the above- identified application.

Also enclosed herewith is statement under 37 CFR section 1.8 (b)(3) by Brenda A. Kantorski, the person signing the certificate of mailing of Exhibit A, attesting on the basis of her own personal knowledge that on March 22, 2004, she signed the certificate of mailing under 37 CFR 1.8(a) that was part of the Amendment of Exhibit A, and deposited the same that day with the United States Postal Service in accordance with certification set forth on the certificate of mailing.

In addition, the Amendment of Exhibit A, as well as the Transmittal Letter that accompanied the amendment at the time of filing, included a statement authorizing the Examiner to charge any fees or credit any balances under 37 CFR §1.17, and 1.16 to Deposit Account No. 02-3038.

Accordingly, Applicant respectfully asserts that: 1) a responsive amendment, transmittal letter and a certificate of mailing were filed on or before the expiration of the statutory three month period ending March 23, 2004 , and 2) that any charges related to the amendment were authorized to be charged to Applicants' attorney's deposit account at the time of filing the amendment of Exhibit A.

In light of the foregoing, Applicants respectfully request that the Examiner enter the amendment attached hereto as Exhibit A and accord the same the mailing date of March 22, 2004. If the Examiner has any questions regarding the amendment, or this communication and Exhibits A-C, he is invited to call Applicant's attorney at the number listed below.

The Examiner is hereby authorized to charge any fees or credit any balances under 37 CFR §1.17, and 1.16 to Deposit Account No. 02-3038.

Respectfully submitted,

Bruce D. Jobse Date: August 9, 2004

Bruce D. Jobse, Esq. Reg. No. 33,518
KUDIRKA & JOBSE, LLP
Customer Number 021127
Tel: (617) 367-4600 Fax: (617) 367-4656

Exhibit A

AMENDMENT	Docket No. L0T9-99-0001

Applicant:	Steven R. Beckhardt, Michael R. O'Brien, Elizabeth A. Lorenson and Douglas W. Conmy
Serial No:	09/431,344
Filed:	October 29, 1999
For:	METHOD AND APPARATUS FOR ENCRYPTING ELECTRONIC MESSAGES COMPOSED USING ABBREVIATED ADDRESS BOOKS
Examiner:	Courtney D. Fields
Art Unit:	2766

CERTIFICATE OF MAILING UNDER 37 C.F.R. §1.8(a)
The undersigned hereby certifies that this document is being placed in the United States mail with first-class postage attached, addressed to Mail Stop Non-Fee Amendment, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on March 22, 2004.

Brenda Kantorski

Mail Stop Non-Fee Amendment
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

In response to the office communication dated December 23, 2003, please amend the above-identified application as follows:

Amendments to the Claims begin on page 2 of this paper.

Remarks/Arguments begin on page 1 of this paper.

Amendments to the Claims

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Original) A method for encrypting an electronic message composed by a sender using an abbreviated address book for delivery over a mail system to a recipient who holds a digital certificate, comprising:

(a) when the sender is off-line, inserting an encryption flag in a header associated with the electronic message;

(b) placing the header and the message in plain text in an outbox;

(c) when the sender is on-line, in response to the flag, requesting the digital certificate from the mail system; and

(d) using the received certificate to encrypt the plain text mail message.

2. (Original) The method according to claim 1 further comprising:

(e) sending the encrypted mail message to the mail system.

3. (Currently Amended) The method according to claim 1 further comprising:

[[(f)]](e) when the sender is on-line, if the flag indicates that the message is encrypted, sending the encrypted mail message to the mail system.

4. (Original) The method according to claim 1 wherein step (c) comprises:

(c1) requesting the digital certificate from the mail system; and

(c2) if the certificate is unavailable, informing the sender that the message cannot be encrypted.

5. (Currently Amended) The method according to claim 4 further comprising:

[[(a)]] (e) sending the unencrypted mail message in the outbox to the mail system when the message cannot be encrypted.

6. (Currently Amended) The method according to claim 1 wherein the header comprises information identifying the recipient and step (c) comprises:

[[(c3)]] (c1) using the identifying information to locate the recipient in the mail system and to retrieve the certificate.

7. (Original) Apparatus for encrypting an electronic message composed by a sender using an abbreviated address book for delivery over a mail system to a recipient who holds a digital certificate, comprising:

a mail composer which inserts an encryption flag in a header associated with the electronic message when the sender is off-line;

a sending mechanism which places the header and the message in plain text in an outbox;

a verification mechanism which is operable when the sender is on-line and, in response to the flag, requests the digital certificate from the mail system; and

an encryption mechanism which uses the received certificate to encrypt the plain text mail message.

8. (Original) The apparatus according to claim 7 further comprising:

an outbox mechanism which sends the encrypted mail message to the mail system.

9. (Original) The apparatus according to claim 7 further comprising:

a mail mechanism which operates when the sender is on-line and, if the flag indicates that the message is encrypted, sends the encrypted mail message to the mail system.

10. (Original) The apparatus according to claim 7 wherein the verification mechanism comprises:

a mechanism which requests the digital certificate from the mail system; and

warning apparatus which informs the sender that the message cannot be encrypted if the certificate is unavailable.

11. (Previously Amended) The apparatus according to claim 10 further comprising:

an outbox mechanism which sends the unencrypted mail message in the outbox to the mail system when the message cannot be encrypted.

12. (Original) The apparatus according to claim 7 wherein the header comprises information identifying the recipient and wherein the verification apparatus comprises: a locator which uses the identifying information to locate the recipient in the mail system and to retrieve the certificate.

13. (Original) A computer program product for encrypting an electronic message composed by a sender using an abbreviated address book for delivery over a mail system to a recipient who holds a digital certificate, the computer program product comprising a computer usable medium having computer readable program code thereon, including:

program code operable when the sender is off-line, for inserting an encryption flag in a header associated with the electronic message;

program code for placing the header and the message in plain text in an outbox;

program code operable when the sender is on-line and, in response to the flag, for requesting the digital certificate from the mail system; and

program code for using the received certificate to encrypt the plain text mail message.

14. (Original) The computer program product according to claim 13 further comprising:

program code for sending the encrypted mail message to the mail system.

15. (Original) The computer program product according to claim 13 further comprising:

program code operable when the sender is on-line and, if the flag indicates that the message is encrypted, for sending the encrypted mail message to the mail system.

16. (Original) The computer program product according to claim 13 wherein the program code for requesting the certificate comprises:

program code for requesting the digital certificate from the mail system; and

program code for informing the sender that the message cannot be encrypted, if the certificate is unavailable.

17. (Original) The computer program product according to claim 16 further comprising:

program code for sending the unencrypted mail message in the outbox to the mail system when the message cannot be encrypted.

18. (Original) The computer program product according to claim 13 wherein the header comprises information identifying the recipient and the program code for requesting the certificate comprises:

program code for using the identifying information to locate the recipient in the mail system and to retrieve the certificate.

19. (Original) A computer data signal embodied in a carrier wave for encrypting an electronic message composed by a sender using an abbreviated address book for delivery over a mail system to a recipient who holds a digital certificate, the computer data signal comprising:

program code operable when the sender is off-line, for inserting an encryption flag in a header associated with the electronic message;

program code for placing the header and the message in plain text in an outbox;

program code operable when the sender is on-line and, in response to the flag, for requesting the digital certificate from the mail system; and

program code for using the received certificate to encrypt the plain text mail message.

20. (Original) The computer data signal according to claim 19 further comprising: program code for sending the encrypted mail message to the mail system.

Remarks and Arguments

Applicants have carefully considered the Office Action dated December 23, 2003 and the references cited therein. Applicants respectfully request reexamination and reconsideration of the application.

Claims 3, 5-6 has been amended to correct limitation numbering. These amendments have not been made to distinguish over any reference of record or for patentability purposes to comply with 35 USC 112. Accordingly, no narrowing of any corresponding equivalents to which these claims are entitled is intended by this amendment.

Claims 14-18 stand rejected under 35 USC Section 102(b) as being anticipated by US Patent 5,552,897, Mandelbaum et al., hereafter "Mandelbaum", already of record. In the prior response, Applicants and their Attorney requested that the Examiner clarify this rejection, as claims 14-18 dependent from independent claim 13 which was rejected under 35 USC Section 103(a). Yet the Examiner has merely reiterated the same rejection. Accordingly, Applicants specifically requested telephone interview with the Examiner and her Supervisory Patent Examiner. And this time, Applicants are left with no other choice but to again respectfully traverse the rejection of claims 14-18 under 35 USC Section 102(b) as improper. Specifically, claims 14-18 include all the limitations of independent claim 13, and, therefore, are more narrow in scope than independent claim 13 from which they depend. Yet claim 13 has been rejected as unpatentable under USC Section 103(a) in light of the combined teachings of Mandelbaum and Kocher. In setting forth the rejection of claim 13, the Examiner admits that Mandelbaum does not explicitly disclose a computer program product used for encrypting electronic message is composed by a sender for delivery over a mail system to a recipient who holds a digital certificate. However, claims 14-18 each explicitly recite a computer program product. Accordingly, Applicants are puzzled how dependent claims 14-18 may be anticipated by Mandelbaum in light of the Examiner's express admission in the deficiency of Mandelbaum's teachings regarding a computer program product. *If the primary reference used by the Examiner admittedly does not teach, suggest or disclose all of the limitations of an independent claim, the dependent claims can not be anticipated by the same primary reference, since the deficiency of the*

primary reference applies equally to all of the dependent claims as well. In light of the foregoing, Applicants submit no further arguments or traversals, at this time, regarding the rejection of claims 14-18, until the Examiner clarifies the rejections thereof.

Before addressing the remaining rejections, Applicants request that the Examiner consider the following. The present invention addresses the need to provide secure electronic mail capabilities to an off-line user. In prior art systems, if a user operating "off-line" attempts to send encrypted electronic mail to a recipient, the recipients digital certificate was typically not available. Accordingly a user could only send encrypted electronic mail messages while on-line. The present invention enables a user to compose electronic mail messages while off-line, and designate such messages to be sent in encrypted format, at a later time once the author of the electronic mail message goes "on-line". The composed, but as yet unencrypted, messages are placed in the mail system outbox with a flag set in the header associated with the message indicating that a digital certificate for encryption is required. Once the user goes online, functionality within the inventive system reviews the electronic mail messages in the outbox. If the value of the encryption flag associated with an unencrypted message indicates that encryption is desired, the recipient information is retrieved and a digital certificate is requested. Once the certificate is received from the recipient, the message can be encrypted. Accordingly, *the present invention enables the composition of electronic mail messages while off-line for encryption at a later time.* Applicants are unaware of any prior art which enables subsequent encryption of previously compose electronic mail messages. None of the prior art cited by the Examiner, whether considered singularly or in combinations, discloses, teaches, or suggest such a system. The Examiner will note that Applicants, in the Background of the Invention of the subject application, have acknowledged that electronic mail systems and the use of digital certificates for encryption thereof prior to sending are already known in the arts.

Claims 1-12 stand rejected under 35 USC Section 102(b) as being anticipated by Mandelbaum. In response, Applicants respectfully reassert all of the remarks and traversals regarding claims 1 and 7, and their respective dependent claims, as set forth in prior response to such rejections. Specifically, the Examiner has failed to indicate where Mandelbaum discloses the limitation of "*requesting the digital certificate from the*

mail system " as recited in claim 1. In addition, Applicants further direct Examiner's attention to the fact that Mandelbaum discloses a system for retrieving facsimile data over a telephone network, not an electronic mail network.

Claims 13, 19 and 20 stand rejected under 35 USC Section 103(a) as being anticipated by Mandelbaum in view of US Patent 5, 903, 651, Kocher. In setting forth the rejection of claims 13, 19 and 20, the Examiner admits that Mandelbaum does not explicitly disclose a computer program product used for encrypting electronic message is composed by a sender for delivery over a mail system to a recipient who holds a digital certificate. Instead, the Examiner is relying on Kocher to disclose such teaching, alleging that Kocher discloses a secure electronic mail system used as an electronic communications protocol allowing the two or more computers or other electronic devices to exchange digital data or messages via a communications channel. Examiner further states that it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of both Mandelbaum and Kocher which will enable a user to compose an off-line message before incorporating a digital certificate which is used to verify messages exchanged via a communications channel.

Applicants traverses the rejection of claims 13 and 19 under 35 U.S.C. §103(a) on the grounds that the Examiner has failed to create a *prima facie* case of obviousness. In accordance with MPEP §2143.03, to establish a *prima facie* case of obviousness 1) the prior art reference (or references when combined) must teach or suggest *all* of the claim limitations; 2) there must be some suggestion or motivation to modify a reference or combine references; and 3) there must be a reasonable expectation of success.

By the own Examiner's admissions of record and for the same reasons as set forth above with respect to the traversal of the claim 1 rejections, Applicants respectfully assert that Mandelbaum does not disclose the subject matter of claims 13 and 19. Specifically, claim 13 is directed to a computer program product for encrypting an electronic message composed by a sender using an abbreviated address book for delivery over a mail system and specifically recites "program code operable when the sender is on-line and, in response to the flag, for requesting the digital certificate from the mail system" (claim 13, lines 9-10). Claim 19 is the computer and data signal

counterparts to claim 13 and recites similar language (claim 19, lines 8-9). Even if all of the assertions made by the Examiner regarding Kocher were true, which Applicant are not admitting to by the statement, Kocher does not teach disclose or suggest the teachings absent from Mandelbaum. Specifically, Kocher discloses nothing more than a system that utilizes a central authority for issuing digital certificates and utilizes private and public encryption keys to enable secure communications. In the present invention when mail is to be sent by an off-line user to a recipient who holds a digital certificate, the sender's electronic mail program allows the sender to compose the mail, but the mail is placed in plain text in the sender's local outbox and flagged for subsequent encryption. When the sender later connects to a mail server to send the outgoing mail, the sender's mail software will request the recipient's certificate from the server and use the received certificate to encrypt the mail message before it leaves the sender's workstation. Accordingly, *the present invention enables the composition of electronic mail messages while off-line for encryption at a later time*. The sections of Kocher cited by the Examiner do not provide a teaching suggestion or disclosure of program code for requesting the digital certificate from the mail system, in response to the value of an encryption flag, *once the sender goes on-line,* as recited in claims 13 and 19. The Examiner's statements regarding the motivation for combining the Mandelbaum and Kocher references are irrelevant in the absence of any teaching or disclosures to support such assertions. Accordingly, Applicants respectfully assert that claims 13 and 19 are believed patentable over the combination of Mandelbaum and Kocher whether considered singularly or in combination.

Claims 14-18 include all the limitations of claim 13 and are likewise believed allowable over the combination of Mandelbaum and Kocher for at least the same reasons as claim 13, as well as for the merits of their own respective limitations. Similarly, claim 20 includes all the limitations of claim 19 and is likewise believed allowable over the combination of Mandelbaum and Kocher for at least the same reasons as claim 19, as well as for the merits of its own respective limitations.

Applicants respectfully reassert all of the remarks and traversals set forth in prior responses to the extent still relevant to the outstanding rejections.

Applicants believe the claims are in allowable condition. A notice of allowance for this application is solicited earnestly. If the Examiner has any further questions regarding this amendment, he/she is invited to call Applicants' attorney at the number listed below. The Examiner is hereby authorized to charge any fees or credit any balances under 37 CFR §1.17, and 1.16 to Deposit Account No. DA-12-2158.

Respectfully submitted,

Date: 3/22/04

Bruce D. Jobse, Esq. Reg. No. 33,518
KUDIRKA & JOBSE, LLP
Customer Number 021127
Tel: (617) 367-4600 Fax: (617) 367-4656